ISSN 2278-3083
Volume 3, No.2, March - April 2014
International Journal of Science and Applied Information Technology
Available Online at http://warse.org/pdfs/2014/ijsait04322014.pdf

Data Accountability in Cloud Using CIA Framework

Prof. Shrikant Dhamdhere, Sachin M., Sagar S., Sayli K., Tejal G.
schnmisal@gmail.com, salunkhesagar96@gmail.com, saylikumbhar31@gmail.com, ghodekar.tejal1@gmail.com.

Abstract: *The major feature of cloud service is that the user's data is processed on remote machines. In this scenario data owner does not know, on which machine his data will get processed. Due to this users fears of losing control of their own data and there are chances that the data may be get changed by an unauthorized users. To avoid this problem we are proposing a framework i.e. Cloud Information Accountability (CIA) framework. This framework will allow the data owner to provide access privileges to users. The framework will also provide the facility of auditing which allows data owner to check the actual usage of their own data. For this purpose Log file will be created whenever the data get accessed and get send to the data owner.*

Keyword: *CIA Framework, Auditing, Log File, Logger, Push Mode, Pull Mode, Certificate Authority.*

1. INTRODUCTION

In today's scenario Cloud Computing is playing very vital role for providing the virtual storage space to users. There are basically three types of cloud.

- Private Cloud
- Public Cloud
- Hybrid Cloud

Private Cloud which is restricted to small organizations. Public Cloud which is used by multiple organizations. And hybrid cloud which is a combination of private cloud and public cloud. By using cloud computing the user's data get processed on remote machine. Due to this user's fears of losing control of their data. Due to this problem we are proposing a Cloud Information Accountability Framework (CIA Framework). This will provide the main feature of auditing which will allow the data owner to check the actual usage of their own data by creating a log file [1]. The log file is a simple file containing the information about the user's whom will access the data of particular user. This log file will get send to the data owner either periodically or as per owner's requirements. Due to this data owners will not fear about losing control of their data. This system can be used in situations where data owner want to track the actual usage of his/her data by using auditing mechanism and log generation. By using CIA framework the system will become more track able.

2. CLOUD INFORMATION ACCOUNTABILITY (CIA)

The main component of CIA framework is Logger component. Figure 1(below) shows the CIA framework in which initially data owner want to publish his own data on cloud server before publishing data, authenticity of data owner is checked with the help of Certificate Authority. Certificate Authority is an entity which is responsible for providing authentication to all users.

Certificate Authority will authenticate the data owner. In CIA we are again considering one special entity which will act like admin which will provide one key to data owner by using this key. Data owner will encrypt his data and publish the encrypted data on the cloud server. This data will be accessed

by end users. User's provides access request to cloud server but before providing response to users their authenticity will be checked by using Certificate Authority. To access this data again the user has to be registered under the entity (admin) in CIA framework.

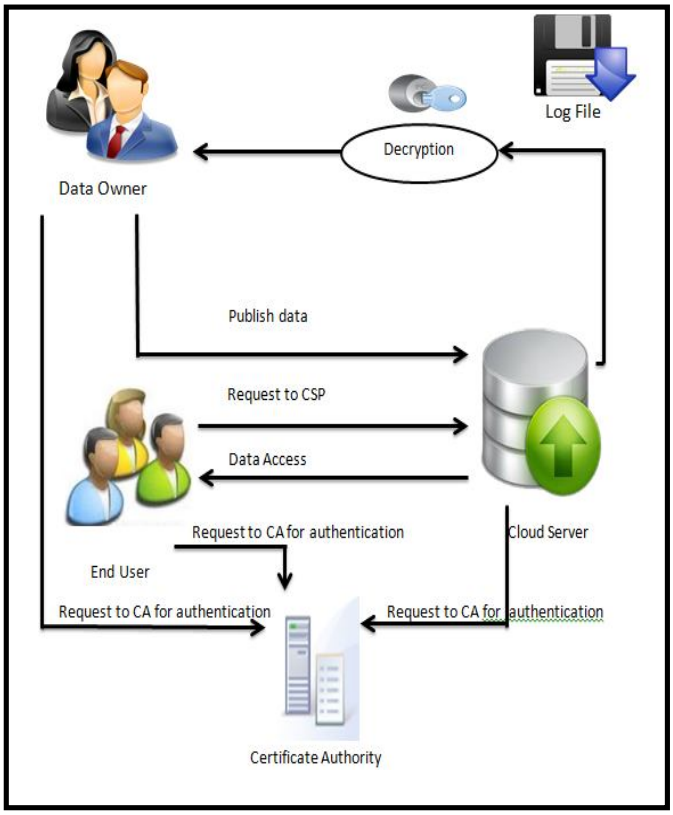

Figure 1. CIA Framework

This entity will provide the key to user. By using this key user can decrypt the file. The data owner and user must be registered under admin (entity in CIA) in order to get key. Certificate entity will provide authentication to users. By using CA, admin concept in CIA and encryption algorithm unauthorized access to data will get avoided. Whenever the data file is accessed by user the log will get generated. This log file will created with the help of logger component. This log file is a file containing the information about the user like User ID, Location where the user has accessed the data etc. This log file will be send to the data owner either periodically or as per data owner's requirement. This log file will be in encrypted format which will decrypted by data owner.

3. LOG FILE STRUCTURE

Log file contains the parameters like User ID, Date, Time, Location [1] etc. This log file is created with the logger component. Log file will be created whenever there will be access to a data file. This log file will get send to data owner.

4. AUDITING MECHANISM

It is a mechanism which allows data owners to check the actual usage of their data with the help of log file. This log file is get retrieved by data owner. There are two modes to retrieve log file.

4.1 Push mode

In push mode the log file will get periodically send to data owner. In push mode user have to provide some constant time period after which the log file will get send to data owner i.e. the data owner have to wait in order to get the log file.

4.2 Pull mode

While in pull mode the log file will be retrieved by data owner as per his requirement. By using pull mode data owner don't have to wait for long period of time as that of in push mode.

5. ACCESS PRIVILEGES

Data owner will be responsible to provide access privileges to users i.e. the data owner will decide which user will be allowed to download a file or will be only able to read a file. For example the person who has not registered to the system will be only able to view the system not able to download it. There can be different types of access privileges like view, download, timely access, location wise access etc. By providing access privileges data owner will able restrict the access of the data.

6. ENCRYPTION ALGORITHM

Advanced Encryption Standard (AES) which is a symmetric key algorithm. In this scenario the key will be generated by a special entity in CIA framework currently we are considering it as an admin. This entity will be responsible in order to provide the key to authenticated users and data owners. With the help of this key, the users will be allowed to access the file.

7. SECURITY DISCUSSION

By using the CA and encryption algorithm we can prevent unauthorized access to data. Even by using log file concept the users can't deny about the access of the data file. Even we can avoid disassembling attack [1]. In this attack, the attacker tries disassemble the file and try to extract important information from the file. This attack can be avoided because of the use of cryptographic mechanism. By using cryptographic mechanism only authorized users will be allowed to access the file.

8. CONCLUSION

The CIA approach of automatically creating a log file allows data owners to check the actual usage of their data. Due to this the data owner will not have to worry about losing the control of his own data.

REFERENCES

[1] S. Sundareswaran, A. Squicciarini, D. Lin. "**Distributed Accountability for Data Sharing in the Cloud**" Proc. IEEE Transactions on Dependable and Secure Computing, Vol. 9, No.4, Aug. 2012

[2] "**Distributed Accountability for Data Sharing in Cloud**" International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012.

[3]. S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, "**Promoting Distributed Accountability in the Cloud**" Proc. IEEE Int'l Conf. Cloud Computing, 2011.

[4] D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigen-baum, J. Hendler, and G.J. Sussman, "**Information Accountability**" Comm. ACM, vol. 51, no. 6, pp. 82-87, 2008.

[5] B.Crispo and G.Ruffo, "**Reasoning about Accountability within Delegation**" Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.